UỶ BAN NHÂN DÂN **XÃ ÁI THƯỢNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 324 /QĐ-UBND	*Ái Thượng, ngày 27 tháng12 năm 2023*

QUYẾT ĐỊNH
Về việc ban hành quy trình ứng cứu xử lý sự cố an toàn thông tin mạng tại Cơ quan xã Ái Thượng

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ ÁI THƯỢNG

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015; Luật sửa đổi; bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức HĐND&UBND địa phương ngày 22/11/2019;

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006;

Căn cứ Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông về việc quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 666/QĐ-STTTT ngày 6/11/2023 của Sở Thông tin & Truyền thông Thanh Hoá về việc phê duyệt cấp độ an toàn hệ thống thông tin UBND huyện Bá Thước, tỉnh Thanh Hóa;

Thực hiện Công văn số 1220/STTTT-CNTT ngày 13/6/2022 của Sở Thông tin & Truyền thông Thanh Hoá về việc đôn đốc các hoạt động triển khai công tác ứng cứu, xử lý sự cố an toàn thông tin mạng.

Theo đề nghị của Công chức Văn phòng – thống kê xã.

QUYẾT ĐỊNH:

Điều 1. Quyết định phê duyệt: Quy trình ứng phó xử lý sự cố an toàn thông tin mạng tại cơ quan xã Ái Thượng.

Điều 2. Giao Công chức Văn phòng – Thống kê xã chủ trì, phối hợp với các ban, ngành, đơn vị, công chức liên quan tổ chức triển khai thực hiện.

Điều 3. Quyết định này có hiệu lực kể từ ngày ký.

Công chức Văn phòng – thống kê, Tài chính – kế toán, Văn hóa – xã hội; các ban, ngành, đơn vị liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3 QĐ;
- Phòng văn hóa thông tin huyện;
- TTr ĐU, HĐND, MTTQ;
- Chủ tịch, các PCT UBND xã;
- Công chức chuyên môn;
- Các đoàn thể;
- Lưu: VT.

CHỦ TỊCH

Nguyễn Đức Lục

Số: 324/QĐ-UBND; 27/12/2023; 7:42:11 +07:00

QUY TRÌNH
Ứng phó xử lý sự cố an toàn thông tin mạng tại Cơ quan xã Ái Thượng

(Ban hành kèm theo Quyết định số: /QĐ-UBND ngày /12/2023 của Chủ tịch UBND xã Ái Thượng)

I. SỰ CẦN THIẾT XÂY DỰNG QUY TRÌNH

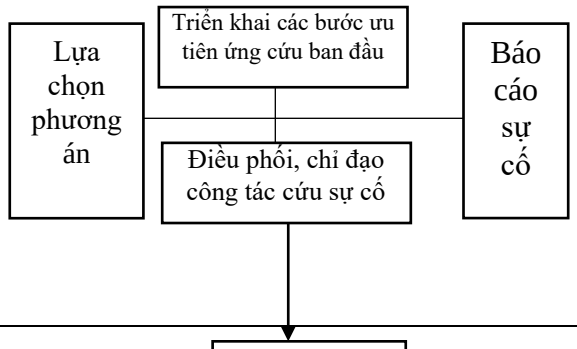
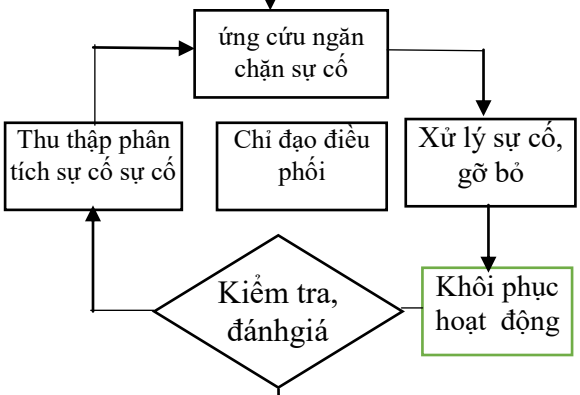
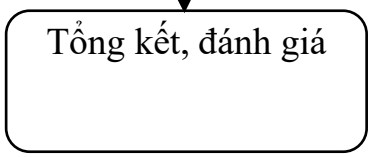
Thế giới bước vào cuộc cách mạng công nghiệp lần thứ tư với sự phát triển mạnh mẽ của không gian mạng đã mang lại những lợi ích to lớn trên nhiều lĩnh vực của đời sống xã hội, làm thay đổi diện mạo mới của nhiều quốc gia, đem lại những thành tựu vượt bậc cho nhân loại. Tuy nhiên, với tính toàn cầu và khả năng kết nối vô hạn của không gian mạng có thể nói không bị giới hạn bởi không gian, thời gian và bản chất xã hội. Không gian mạng cũng đặt ra nhiều thách thức rất lớn đối với an ninh của các quốc gia trên thế giới như: Chiến tranh mạng, chiến tranh thông tin, khủng bố mạng, tội phạm mạng…vấn đề phát triển và làm chủ không gian mạng đã trở thành một trong những nhiệm vụ cấp bách được nhiều quốc gia đặc biệt quan tâm. Chính vì vậy, bảo đảm an ninh mạng đang là ưu tiên hàng đầu được thể hiện rõ trong các quan điểm, chiến lược và hành động cụ thể của các quốc gia, trong đó có Việt Nam.

Để đảm bảo an toàn thông tin, an ninh quốc gia thì mỗi cơ quan hành chính Nhà nước cần thực hiện các biện pháp đảm bảo an toàn thông tin, an ninh mạng trong hệ thống nội bộ. Do hệ thống an toàn thông tin trong các cơ quan nhà nước còn nhiều hạn chế, nên có nhiều vụ tấn công trên mạng và các vụ xâm nhập hệ thống công nghệ thông tin nhằm do thám, phá hoại dữ liệu, ăn cắp tài sản... và một số vụ việc mất an toàn thông tin khác gia tăng ở mức báo động về số lượng, đa dạng về hình thức, tinh vi hơn về công nghệ.

Do đó, việc xây dựng quy trình ứng phó xử lý sự cố an toàn thông tin mạng tại Cơ quan xã Ái Thượng là thực sự cần thiết.

II. QUY TRÌNH CHUNG XỬ LÝ CÁC SỰ CỐ VÀ BẢO ĐẢM ATTT TẠI CƠ QUAN XÃ ÁI THƯỢNG: Theo sơ đồ sau:

Thành phần	Quy trình	Ghi chú
- Đơn vị vận hành Hệ thống thông tin: Văn phòng – Thống kê xã	Phát hiện, tiếp nhận thông báo sự cố	Thông tin sự cố có thể từ các nguồn: -Nguồn tin xã hội; - Hacker tấn công; - Sử dụng thiết bị ngoại vi không an toàn: USB, ổ cứng di động…
- Đơn vị vận hành Hệ thống thông tin: Văn phòng – thống kê	Phân tích, xác minh sự cố Chưa xảy ra Phản hồi, kết thúc Đã xảy ra	Đơn vị thường trực về ứng cứu sự cố: Quản trị mạng và các bộ phận liên quan.

<table>
<tr>
<td>- Quản trị mạng cơ quan UBND xã triển khai các bước ứng cứu, xử lý ban đầu; báo cáo sơ bộ sự cố.
- Báo cáo lãnh đạo Văn phòng phối hợp với Tổ ứng cứu CNTT của huyện xử lý (nếu cần)</td>
<td> 
</td>
<td>Triển khai theo phương án đối phó, ứng cứu một số tình huống sự cố cụ thể hoặc theo hướng dẫn của đơn vị thường trực về ứng cứu sự cố của tỉnh.</td>
</tr>
<tr>
<td>- Tổ chức triển khai hoặc phối hợp với Tổ ứng cứu CNTT của huyện thực hiện phân tích, xác định nguồn gốc tấn công để tổ chức ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.</td>
<td> 
</td>
<td>Các thành phần tham gia ứng cứu sự cố căn cứ nội dung, nhiệm vụ được giao theo phân công, chỉ đạo tổ chức triển khai các quy trình, nghiệp vụ của mình. quy trình này được triển khai liên tục, đảm bảo đến khi khôi phục hoạt động của hệ thống thông tin trở lại bình thường.</td>
</tr>
<tr>
<td>- Đơn vị vận hành Hệ thống: Văn phòng – thống kê xã.
- Cơ quan thường trực về ứng cứu sự cố an toàn thông tin mạng của huyện.</td>
<td> 
</td>
<td></td>
</tr>
</table>

Trong đó, các bước triển khai, bao gồm:

1. Phát hiện, tiếp nhận, ứng cứu ban đầu và thông báo sự cố

1.1. Phát hiện, tiếp nhận, xác minh sự cố

Đơn vị vận hành hệ thống thông tin (Văn phòng – thống kê xã) chủ trì, là bộ phận thường trực về ứng cứu sự cố của cơ quan xã và các phòng, ban liên quan tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố từ các nguồn bên trong và bên ngoài (cảnh báo sự cố: Văn bản, email, điện thoại, website, mạng xã hội...; phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá). Khi xác định được sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp.

Các loại sự cố chính, bao gồm:

- Sự cố do bị tấn công hệ thống mạng;
- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền...;
- Sự cố do lỗi của người quản trị, vận hành hệ thống;
- Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn…
- Sự cố do lỗi của người sử dụng.

1.2. Triển khai, lựa chọn các bước ưu tiên ứng cứu ban đầu

Sau khi đã xác định sự cố xảy ra, bộ phận Quản trị mạng cơ quan xã thông tin tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố theo phương án đối phó, ứng cứu một số tình huống sự cố cụ thể tại ***Mục II*** hoặc theo tư vấn, hướng dẫn của Cơ quan thường trực về ứng cứu sự cố của huyện.

1.3. Thông báo, báo cáo sự cố

Sau khi triển khai các bước ưu tiên ứng cứu ban đầu, Quản trị mạng cơ quan xã thực hiện thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan, tổ chức theo quy định. Cụ thể:

- Thông báo cho Văn phòng – thống kê xã, các phòng, ban, cơ quan sử dụng chung hệ thống mạng LAN trong cơ quan xã và đơn vị thường trực về ứng cứu sự cố của tỉnh chậm nhất 02 ngày kể từ khi phát hiện sự cố; trường hợp xác định sự cố có thể vượt khả năng xử lý, quản trị mạng cơ quan xã tham mưu cho Chủ tịch UBND xã báo cáo ban đầu sự cố bằng văn bản về đơn vị thường trực về ứng cứu sự cố của tỉnh.

- Hình thức gửi báo cáo: Văn phòng – thống kê xã gửi báo cáo về đơn vị thường trực về ứng cứu sự cố của tỉnh theo một trong 2 hình thức sau:

+ Qua đường văn bản: Gửi về Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa.

+ Qua hộp thư điện tử: Gửi về địa chỉ: ungcuusuco@thanhhoa.gov.vn

1.4. Điều phối công tác ứng cứu

- Căn cứ vào tính chất sự cố, đề nghị hỗ trợ của cơ quan xã và báo cáo ban đầu của đơn vị thường trực về ứng cứu sự cố của tỉnh. Đội ứng cứu sự cố của tỉnh thực hiện công tác điều phối, giám sát cơ chế phối hợp, chia sẻ thông tin theo phạm vi, chức năng, nhiệm vụ của mình để huy động nguồn lực ứng cứu sự cố.

- Hướng dẫn thực hiện yêu cầu điều phối xử lý sự cố tới các thành viên trong Đội ứng cứu sự cố của tỉnh chi tiết tại ***Mục III***.

2. Triển khai ứng cứu, ngăn chặn sự cố

Công chức Văn phòng – thống kê phối hợp với đơn vị thường trực về ứng cứu sự cố của huyện, tỉnh và các đơn vị liên quan tiến hành triển khai theo phương án đối phó, ứng cứu một số tình huống sự cố cụ thể tại ***Mục II***. Trong đó, tập trung nguồn lực thực hiện:

2.1. Triển khai thu thập chứng cứ, xác định phạm vi, đối tượng bị ảnh hưởng

- Thu thập thông tin ban đầu để phục vụ phân tích sự cố:

+ Thông tin về đầu mối liên hệ;

+ Thu thập thông tin hệ thống;

+ Thu thập chức năng của hệ thống;

+ Thu thập cấu hình của hệ thống (OS, Service, version, network...);

+ Thu thập chứng cứ;

+ Thu thập bộ nhớ;

+ Thu thập trạng thái network và các kết nối;

+ Thu thập các tiến trình đang chạy;

+ Thu thập hard driver media;

+ Thu thập log file;

+ Thu thập các cổng đang mở của hệ thống.

2.2. Triển khai phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin

- Phân tích sự cố, xác định nguồn gốc tấn công

+ Phân tích dòng thời gian;

+ Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi;

+ Thời gian thực hiện các cập nhật lớn đối với hệ thống;

+ Thời điểm mà hệ thống sử dụng lần cuối cùng;

- Phân tích dữ liệu

+ Phân tích các máy trạm chứa tệp (File System);

+ Phân tích Resgitry;

+ Phân tích Windows;

+ Phân tích kết nối mạng;

3. Xử lý sự cố, gỡ bỏ và khôi phục

3.1. Xử lý sự cố, gỡ bỏ

Sau khi đã triển khai ngăn chặn sự cố, Văn phòng – thống kê xã và đơn vị thường trực về ứng cứu sự cố của huyện, tỉnh và các đơn vị liên quan triển khai tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin.

3.2. Khôi phục

Văn phòng – thống kê xã chủ trì phối hợp với các đơn vị liên quan triển khai các hoạt động khôi phục hệ thống thông tin dữ liệu và kết nối; cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng phần mềm bảo đảm an toàn thông tin cho hệ thống thông tin.

3.3. Kiểm tra, đánh giá hệ thống thông tin

Văn phòng – thống kê xã và các đơn vị liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống chưa hoạt động ổn định, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và tổ chức các bước tương ứng để xử lý dứt điểm, khôi phục hoạt động bình thường của hệ thống thông tin.

4. Tổng kết, đánh giá

4.1. Tổng kết, đúc rút kinh nghiệm

Văn phòng – thống kê xã phối hợp với đơn vị thường trực về ứng cứu sự cố của huyện, tỉnh triển khai tổng hợp tất cả các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai, báo cáo cơ quan chuyên trách về an toàn thông tin của tỉnh; tổ chức phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai...

4.2. Xây dựng báo cáo kết thúc ứng phó sự cố

Văn phòng – thống kê xã, bộ phận thường trực về ứng cứu sự cố của xã triển khai tổng hợp và xây dựng báo cáo kết thúc ứng phó sự cố, trong đó trình bày chi tiết quá trình xử lý sự cố, tóm tắt tổng quát về tình hình sự cố và đề xuất cách thức triển khai điều phối, ứng cứu sự cố nhằm xử lý nhanh, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự.

Sau khi kết thúc ứng cứu sự cố, trong vòng 10 ngày Văn phòng – thống kê xã xây dựng báo cáo kết thúc ứng phó sự cố, gửi về cơ quan chuyên trách về an toàn thông tin của huyện, tỉnh./.

III. QUY TRÌNH CHI TIẾT XỬ LÝ CÁC SỰ CỐ VÀ BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG:

1. Sự cố rò rỉ dữ liệu

Bước	Nội dung tham khảo thực hiện	Bộ phận thực hiện
Dấu hiệu	- Dữ liệu của cơ quan bị rò rỉ, phát tán trên không gian mạng - Tài khoản truy cập vào các hệ thống phần mềm dùng chung bị chiếm đoạt, khai thác trái phép. - Dữ liệu bị thay đổi, xóa bỏ, lấy cắp trái phép	Quản trị mạng
Xử lý ưu tiên, ban đầu	- Cô lập hệ thống: Tách máy tính, thiết bị nghi ngờ rò rỉ dữ liệu ra khỏi hệ thống mạng nội bộ và ngắt kết nối Internet. - Tiến hành xác minh nhanh dữ liệu bị rò rỉ, xác định mức độ và phạm vi rò rỉ dữ liệu.	
Xác định nguyên nhân, đánh giá tác động của sự cố và xử lý ban đầu.	- Từ những dấu hiệu, thông tin thu được khoanh vùng nguyên nhân, nguồn gốc của sự cố. Nếu sự cố liên quan đến băng thông, xử lý theo bước tiếp theo. Nếu sự cố liên quan đến tấn công DdoS - Distributed Denial of Service (Tấn công từ chối dịch vụ phân tán), xử lý theo quy trình tấn công mạng. - Thông báo đơn vị thường trực về ứng cứu sự cố của tỉnh về mức độ, phạm vi ảnh hưởng ban đầu và thời gian dự kiến khắc phục của sự cố (nếu tự khắc phục được). - Đánh giá sơ bộ về thiệt hại hoặc mức độ ảnh hưởng của sự cố hoặc phối hợp với đơn vị thường trực về ứng cứu sự cố của huyện, tỉnh để thực hiện đánh giá.	Văn phòng – thống kê xã / Quản trị mạng/ Trung tâm ƯCSC tỉnh/ Các đơn vị liên quan
Cô lập hệ thống	- Thực hiện cô lập hệ thống bị tấn công để tránh bị thay đổi hiện trường. - Thông báo tới đơn vị thường trực về ứng cứu sự cố của huyện, tỉnh để hỗ trợ.	
Xử lý sự cố	- Xác định nguyên nhân của sự cố an ninh mạng. - Rà soát hệ thống để phát hiện các lỗ hổng có thể bị khai thác tấn công vào cơ sở dữ liệu. - Rà soát khả năng lộ mật khẩu của các tài khoản quản trị, tài khoản có quyền quản trị cơ sở dữ liệu. - Rà quét và xử lý mã độc trên máy tính của người sử dụng các tài khoản này, thay đổi mật khẩu các tài khoản.	

Khôi phục hệ thống	- Xác định được lỗ hổng mà hacker đã sử dụng để tấn công, thực hiện vá các lỗ hổng này. - Rà soát và vá các lỗ hổng ở module khác của hệ thống. - Sử dụng các công cụ rà quét mạng để phát hiện bất kỳ truy cập nào trái phép hoặc phát hiện sự quay trở lại của hacker.	Quản trị mạng/ Các đơn vị liên quan
Kiện toàn hệ thống	- Báo cáo lại toàn bộ các thông tin liên quan đến sự cố như cách thức phát hiện, đánh giá, xử lý sự cố và khôi phục hệ thống để làm tài liệu tham khảo cho các lần sau. - Đánh giá, tổng kết sự cố để hoàn thiện phương án. - Phối hợp các cơ quan chức năng để phối hợp mở rộng phạm vi.	Văn phòng – thống kê xã /Lãnh đạo Cơ quan

2. Sự cố tấn công thay đổi giao diện

Bước	Nội dung tham khảo thực hiện	Bộ phận thực hiện
Dấu hiệu	Cổng thông tin điện tử xã Ái Thượng bị thay đổi trái phép nội dung toàn bộ hoặc một phần.	Văn hóa – xã hội
Xử lý ưu tiên, ban đầu	- Thông báo cho Ban biên tập Cổng thông tin điện tử xã - Thông báo cho Văn phòng HĐND&UBND huyện. - Kích hoạt hệ thống dự phòng hoặc trang thông báo lỗi, bảo trì.	
Xác định nguyên nhân, đánh giá tác động của sự cố và xử lý ban đầu.	- Từ những dấu hiệu, thông tin thu được khoanh vùng nguyên nhân, nguồn gốc ban đầu của cuộc tấn công. - Phối hợp kiểm tra xem tên miền có trỏ đúng vào máy chủ web hay không, liên hệ với đơn vị quản lý tên miền để xác định trạng thái tài khoản quản lý tên miền. - Trong trường hợp tên miền không bị chiếm quyền điều khiển: Thực hiện thay thế nội dung trang chủ bằng thông báo bảo trì, nâng cấp hệ thống. - Trong trường hợp tên miền bị chiếm quyền điều khiển: + Yêu cầu lấy lại quyền điều khiển tên miền + Cấu hình tên miền trỏ đúng về địa chỉ máy chủ web. + Yêu cầu khóa tài khoản quản lý tên miền này, không cho phép cập nhật các thông tin liên quan. - Thông báo với các đơn vị liên quan mức độ, phạm vi ảnh hưởng ban đầu và thời gian dự kiến khắc phục của sự cố.	Ban biên tập Cổng Thông tin điện tử xã Ái Thượng / Quản trị website/ Văn phòng – thống kê xã /Các đơn vị liên quan
Cô lập hệ thống	- Thực hiện cô lập hệ thống bị tấn công để tránh bị thay đổi hiện trường. - Rà soát khả năng bị tấn công khai thác của hệ thống dự phòng và chuyển đổi sang hệ thống dự phòng. - Tạm ngắt các tài khoản quản trị, tài khoản có quyền	

	đăng bài lên website. - Thông báo tới các cơ quan chức năng và đối tác để hỗ trợ.	
Xử lý sự cố	- Xác định nguyên nhân của sự cố an ninh mạng. - Phối hợp với Văn phòng UBND tỉnh là đơn vị cung cấp dịch vụ và lưu trữ hosting của website xã thực hiện điều tra, phân tích hệ thống để tìm kiếm các shell, file lạ, phân tích hành vi và xác định nguyên nhân của cuộc tấn công. - Thu thập tất cả các thành phần file độc hại và phối hợp với các đối tác phân tích, điều tra. - Phân tích các hành vi của shell và mã độc. - Xác định và xử lý được đầy đủ các thành phần của mã độc + File shell hacker đã tải lên server + Tiến trình của mã độc + File của mã độc + Thành phần đăng ký khởi động cùng server của mã độc - Rà soát khả năng lộ mật khẩu của các user quản trị, user có quyền đăng bài lên website. - Rà quét và xử lý mã độc trên máy tính của user này, sau đó đổi mật khẩu các user.	
Khôi phục hệ thống	- Điều tra chi tiết hơn về sự cố để mở rộng phạm vi và chống các ảnh hưởng tiềm tàng khác. - Ghi lại toàn bộ các thông tin liên quan đến sự cố như cách thức phát hiện, đánh giá, xử lý sự cố và khôi phục hệ thống để làm tài liệu tham khảo cho các lần sau. -Phối hợp các cơ quan chức năng để phối hợp mở rộng phạm vi.	Quản trị website/ Các đơn vị liên quan

3. Tấn công mã độc

Bước	Nội dung tham khảo thực hiện	Bộ phận thực hiện
Dấu hiệu	Hệ thống mạng LAN/máy tính trong cơ quan xã Ái Thượng bị tấn công bởi các dạng mã độc khác nhau.	Văn phòng – thống kê xã / Quản trị mạng
Xử lý ưu tiên, ban đầu	- Triệu tập Quản trị mạng cơ quan xã Ái Thượng. - Ưu tiên cô lập toàn bộ các máy bị lây nhiễm hoặc có dấu hiệu bất thường. - Kiểm tra các máy tính có dữ liệu quan trọng, cô lập và có biện pháp sao lưu dữ liệu.	

Xác định nguyên nhân, đánh giá tác động của sự cố và xử lý ban đầu.	- Từ những dấu hiệu, thông tin thu được khoanh vùng nguyên nhân, nguồn gốc ban đầu của cuộc tấn công. - Xác định cấu phần thuộc hệ thống bị ảnh hưởng/phạm vi bị ảnh hưởng. - Phối hợp thông báo với tới đơn vị thường trực về ứng cứu sự cố của huyện, tỉnh để hỗ trợ; các đơn vị liên quan mức độ, phạm vi ảnh hưởng ban đầu và thời gian dự kiến khắc phục của sự cố.	Văn phòng – thống kê xã / quản trị mạng/ Các đơn vị liên quan
Cô lập hệ thống	- Thực hiện cô lập hệ thống bị tấn công để tránh bị thay đổi hiện trường và thông báo về khoảng thời gian tạm dừng hệ thống dự kiến. - Thông báo tới đơn vị thường trực về ứng cứu sự cố của tỉnh để hỗ trợ.	
Xử lý sự cố	- Xác định nguyên nhân của sự cố an ninh mạng. - Điều tra, phân tích hệ thống để tìm kiếm các shell, file lạ, phân tích hành vi của nó và xác định nguyên nhân của cuộc tấn công. - Thu thập tất cả các thành phần file độc hại và phối hợp với đơn vị thường trực về ứng cứu sự cố của tỉnh để phân tích, điều tra. - Phân tích các hành vi của shell và mã độc. - Xác định và xử lý được đầy đủ các thành phần của mã độc + File shell hacker đã tải lên + Tiến trình của mã độc + File của mã độc + Thành phần đăng ký khởi động cùng hệ điều hành của mã độc - Rà soát khả năng lộ mật khẩu của các tài khoản người sử dụng trên hệ thống. - Rà quét và xử lý mã độc trên máy tính của các người dùng sử dụng tài khoản này, thay đổi mật khẩu các tài khoản.	
Khôi phục hệ thống	- Xác định được lỗ hổng mà hacker đã sử dụng để tấn công, thực hiện update và vá các lỗ hổng này. - Thực hiện ngăn chặn mã hash, C&C server (Command and Control server – Máy chủ ra lệnh kiểm soát) trong hệ thống Antivirus, Firewall, IPS - Intrusion prevention system (Hệ thống phòng chống xâm nhập). - Đưa hệ thống chính quay lại hoạt động. - Sử dụng các công cụ rà quét mạng để phát hiện bất kỳ truy cập nào trái phép hoặc phát hiện sự quay trở lại của hacker.	Quản trị mạng/ Các đơn vị liên quan
Kiện toàn hệ thống	- Điều tra chi tiết hơn về sự cố để mở rộng phạm vi và chống các ảnh hưởng tiềm tàng khác. - Ghi lại toàn bộ các thông tin liên quan đến sự cố như cách thức phát hiện, đánh giá, xử lý sự cố và khôi phục	

	hệ thống để làm tài liệu tham khảo cho các lần sau. - Phối hợp với đơn vị thường trực về ứng cứu sự cố của tỉnh để phối hợp mở rộng phạm vi.	

4. Tấn công từ chối dịch vụ

Bước	Nội dung tham khảo thực hiện	Bộ phận thực hiện
Dấu hiệu	Toàn bộ các truy cập vào hệ thống mạng LAN Cơ quan xã Ái Thượng không truy cập được hoặc truy cập chậm, gián đoạn.	Quản trị mạng
Xử lý ưu tiên, ban đầu	- Văn phòng – thống kê xã - Thông báo tới Trung tâm Viễn thông Bá Thước - nhà cung cấp dịch vụ và Đội ứng cứu sự cố an toàn thông tin mạng của huyện, tỉnh.	
Xác định nguyên nhân, đánh giá tác động của sự cố và xử lý ban đầu.	- Từ những dấu hiệu, thông tin thu được khoanh vùng nguyên nhân, nguồn gốc ban đầu của cuộc tấn công. - Thông báo với Đội ứng cứu sự cố an toàn thông tin mạng của huyện,tỉnh về mức độ, phạm vi ảnh hưởng ban đầu và thời gian dự kiến khắc phục của sự cố (nếu tự xử lý được).	Văn phòng – thống kê xã / quản trị mạng/ Các đơn vị liên quan
Cô lập hệ thống	- Rà soát khả năng bị tấn công khai thác của hệ thống dự phòng và chuyển đổi sang hệ thống dự phòng. - Trong trường hợp hệ thống dự phòng cũng bị tấn công, thực hiện trỏ tên miền hệ thống thông báo dịch vụ.Đồng thời thực hiện triển khai hệ thống mới tách biệt với hệ thống hiện có về đường truyền, bảo đảm cung cấp các dịch vụ thiết yếu trong thời gian khôi phục hệ thống chính. - Thông báo tới Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh Trung tâm Viễn thông Bá Thước để hỗ trợ.	
Xử lý sự cố	- Xác định nguyên nhân của sự cố an ninh mạng. - Trường hợp Trung tâm Viễn thông Bá Thước, phân giải tên miền bị tấn công từ chối dịch vụ, thực hiện chuyển sang các đường truyền của nhà cung cấp dịch vụ khác. - Liệt kê các địa chỉ IP thực hiện tấn công từ chối dịch vụ và chặn trên hệ thống Firewall; phối hợp Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và Trung tâm Viễn thông Bá Thước thực hiện cấu hình trên hệ thống Firewall ngăn chặn truy cập có IP nguồn từ nước ngoài để giảm thiểu nguồn tấn công và xử lý sự cố.	

Khôi phục hệ thống	- Xác định được lỗ hổng mà hacker đã sử dụng để tấn công, vá các lỗ hổng này. - Rà soát và vá các lỗ hổng ở module khác của hệ thống. - Đưa hệ thống chính quay lại hoạt động. - Sử dụng các công cụ rà quét mạng để phát hiện bất kỳ truy cập nào trái phép hoặc phát hiện sự quay trở lại của hacker.	Quản trị mạng/ Các đơn vị liên quan phối hợp
Kiện toàn hệ thống	- Điều tra chi tiết hơn về sự cố để mở rộng phạm vi và chống các ảnh hưởng tiềm tàng khác. - Ghi lại toàn bộ các thông tin liên quan đến sự cố như cách thức phát hiện, đánh giá, xử lý sự cố và khôi phục hệ thống để làm tài liệu tham khảo cho các lần sau. - Phối hợp Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và Trung tâm Viễn thông Bá Thước để phối hợp mở rộng phạm vi.	

IV. HƯỚNG DẪN THỰC HIỆN YÊU CẦU ĐIỀU PHỐI XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Đơn vị vận hành hệ thống thông tin; đơn vị chủ quản hệ thống thông tin (Văn phòng – thống kê xã) có trách nhiệm tiếp nhận thông tin và yêu cầu điều phối, xử lý sự cố từ Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh, cụ thể như sau:

Bước 1: Đội ứng cứu sự cố gửi yêu cầu điều phối, xử lý sự cố

Trung tâm Công nghệ thông tin và Truyền thông (*cơ quan thường trực của đội ứng cứu sự cố*) gửi yêu cầu điều phối xử lý sự cố tới cơ quan HĐND&UBND huyện Bá Thước dưới các hình thức:

a) Gửi bằng Văn bản

Yêu cầu điều phối xử lý sự cố sẽ được gửi đến cơ quan HĐND&UBND huyện theo đường công văn. Đối với một số trường hợp quan trọng, sẽ gửi văn bản dưới dạng "MẬT" theo quy định.

b) Gửi bằng thư điện tử

- Yêu cầu điều phối xử lý sự cố sẽ được gửi đến Cơ quan HĐND&UBND huyện từ thư điện tử: *ungcuusuco@thanhhoa.gov.vn* với tiêu đề thư "***[ĐƯCSC] Yêu cầu điều phối, xử lý sự cố [tên gọi của sự cố]***".

Bước 2: Tiếp nhận yêu cầu điều phối, xử lý sự cố

Cơ quan HĐND&UBND huyện có trách nhiệm phản hồi lại ngay cho Trung tâm CNTT và Truyền thông qua địa chỉ: *ungcuusuco@thanhhoa.gov.vn* để xác nhận thông tin đã nhận được yêu cầu điều phối đồng thời thực hiện các bước xác minh sự cố và xử lý ban đầu.

Bước 3: Xử lý sự cố

- Văn phòng – thống kê xã thực hiện xử lý sự cố theo quy trình được hướng dẫn tại ***Mục II*** trong công văn này.

- Nếu gặp khó khăn trong quá trình xử lý sự cố, Quản trị mạng cơ quan xã có thể trao đổi thông tin trên kênh chat riêng của Đội ứng cứu sự cố (thiết lập qua ứng dụng Telegram) hoặc có đề xuất Trung tâm Công nghệ thông tin và Truyền thông phối hợp để được hỗ trợ.

Bước 4: Báo cáo kết quả xử lý sự cố

a) Sau khi hết thời gian quy định trong yêu cầu điều phối, xử lý sự cố, Văn phòng – thống kê xã báo cáo kết quả xử lý sự cố về Trung tâm Công nghệ thông tin và Truyền thông, bao gồm:

- Trạng thái sự cố: tồn tại/không còn tồn tại.
- Tình trạng xử lý: đã xử lý xong/đang xử lý/chưa xử lý.
- Thời gian xử lý xong sự cố (nếu sự cố đã được xử lý):
- Đánh giá về yêu cầu điều phối, xử lý sự cố của Trung tâm Công nghệ thông tin và Truyền thông bao gồm:

+ Tính kịp thời: kịp thời/không kịp thời;

+ Tính hiệu quả: hiệu quả/không hiệu quả;

+ Tính chính xác: chính xác/không chính xác;

+ Mức độ hỗ trợ trong quá trình xử lý sự cố của Trung tâm Công nghệ thông tin và Truyền thông: cao/thấp/trung bình/không hỗ trợ;

+ Đề xuất, kiến nghị (nếu có).

b) Hình thức gửi báo cáo: Văn phòng – thống kê xã gửi báo cáo về Trung tâm Công nghệ thông tin và Truyền thông theo một trong 2 hình thức sau:

- Qua đường văn bản: Gửi về Trung tâm Trung tâm Công nghệ thông tin và Truyền thông qua hệ thống phần mềm quản lý văn bản và hồ sơ công việc.
- Qua hộp thư điện tử: ungcuusuco@thanhhoa.gov.vn.